

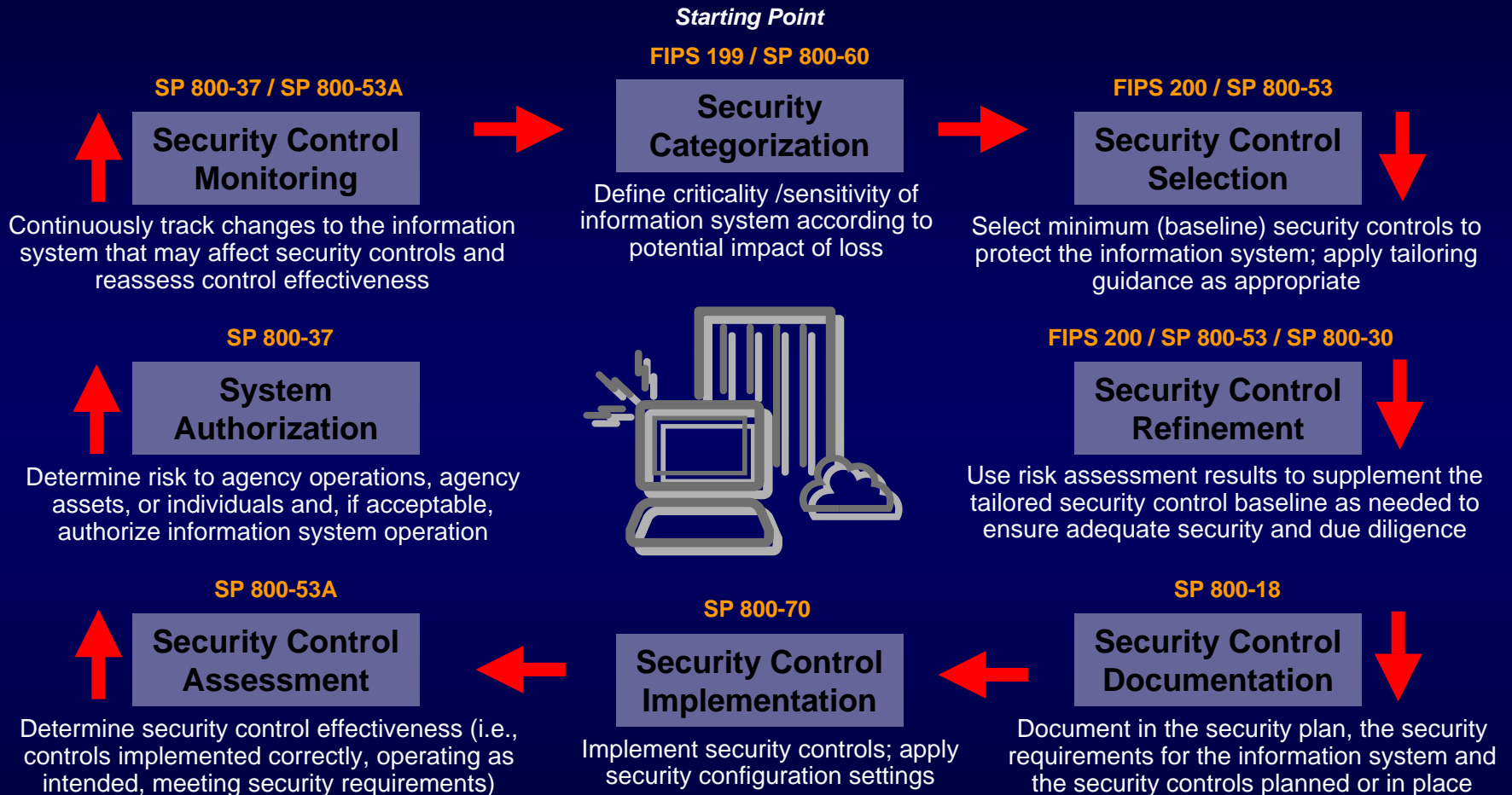
# NIST Risk Framework

*Computer Security Division  
Information Technology Laboratory*

# Managing Enterprise Risk

- Key activities in managing **enterprise-level risk**—risk resulting from the operation of an information system:
  - ✓ **Categorize** the information system (criticality/sensitivity)
  - ✓ **Select** and tailor minimum (baseline) security controls
  - ✓ **Supplement** the security controls based on risk assessment
  - ✓ **Document** security controls in system security plan
  - ✓ **Implement** the security controls in the information system
  - ✓ **Assess** the security controls for effectiveness
  - ✓ **Determine** agency-level risk and risk acceptability
  - ✓ **Authorize** information system operation
  - ✓ **Monitor** security controls on a continuous basis

# The Risk Framework



# Information Security Program

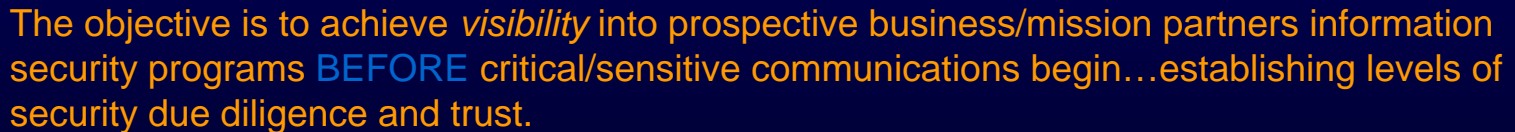


## Links in the Security Chain: Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning
- ✓ Security policies and procedures
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Physical security
- ✓ Personnel security
- ✓ Certification, accreditation, and security assessments
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls and network security mechanisms
- ✓ Intrusion detection systems
- ✓ Security configuration settings
- ✓ Anti-viral software
- ✓ Smart cards

Adversaries attack the weakest link...where is yours?

## Security Visibility Among Business/Mission Partners



# Key Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Management)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)

*Many other FIPS and NIST Special Publications provide security standards and guidance supporting the FISMA legislation...*

# Contact Information

100 Bureau Drive Mailstop 8930  
Gaithersburg, MD USA 20899-8930

## *Project Leader*

Dr. Ron Ross  
(301) 975-5390  
[ron.ross@nist.gov](mailto:ron.ross@nist.gov)

## *Administrative Support*

Peggy Himes  
(301) 975-2489  
[peggy.himes@nist.gov](mailto:peggy.himes@nist.gov)

## *Senior Information Security Researchers and Technical Support*

Marianne Swanson  
(301) 975-3293  
[marianne.swanson@nist.gov](mailto:marianne.swanson@nist.gov)

Dr. Stu Katzke  
(301) 975-4768  
[skatzke@nist.gov](mailto:skatzke@nist.gov)

Pat Toth  
(301) 975-5140  
[patricia.toth@nist.gov](mailto:patricia.toth@nist.gov)

Arnold Johnson  
(301) 975-3247  
[arnold.johnson@nist.gov](mailto:arnold.johnson@nist.gov)

Matt Scholl  
(301) 975-2941  
[matthew.scholl@nist.gov](mailto:matthew.scholl@nist.gov)

Information and Feedback  
Web: [csrc.nist.gov/sec-cert](https://csrc.nist.gov/sec-cert)  
Comments: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)